SECURITY ASSIGNMENT

Edward Snowden, a former contractor for the CIA, fled the US after leaking the details of extensive internet and phone surveillance by intelligence agencies of the public at large.

The numerous intelligence agencies tapp directly into the servers of internet firms, including Facebook, Google, Microsoft and Yahoo, to track online communication in a surveillance programme known as Prism.

These spy agencies also tap fibre-optic cables that carry global communications and share this vast amount of data with other intelligence agencies abroad.

The information from internet and phone use are stored at data centres - like the one in Sahali in Kamloops. There the data is sifted and analyzed.

Snowden also pointed out the double standards implicit in the surveillance: how top-level officials in the military industrial complex committed huge crimes but still managed to get off scot-free, compared to common people who are under close monitoring and claustrophobic surveillance.

This dragnet surveillance can be and is being easily abused by bad actors. AND since it is so useful to globalist entities - it is not going away. Those who are pushing the globalist agenda are using it to ferret out dissidents to their agendas.

Billions of people are inseparable from their phones. Their devices are within reach – and earshot – for almost every daily experience. Few pause to think that their phones can be transformed into surveillance devices, with someone thousands of miles away silently extracting their messages, photos and location, activating their microphone to record them in real time. Entering this information into computers which statistically analyze outcomes.

Such are the capabilities of Pegasus, the spyware manufactured by NSO Group, the Israeli purveyor of weapons of mass surveillance. It is really a one-sided spy game, they have full unfettered access to all your data, surfing, conversations, movements and we have no access to their activities unless their security is breached.

This same easy access to your data is going to be used to track you for a vaccine passport system - to be used as instruments of repression for an authoritarian regime. To track your movements for contact tracers and eventually the QR code will embody not only your vaccine status but also your Chinese style social credit score and carbon tax.

YOU MUST FIGHT THIS AND PROTECT YOUR DATA AND PRIVACY NOW!

Assignment is to install Tor on your computer and your cell phone.
Tor is a software which encrypts your data.

1. Go to https://tb-manual.torproject.org/installation/
2. Follow the directions to get Tor Browser on your computer. Use this Tor browser to surf the internet.
3. Go to the iPhone App Store if you own an iphone OR the Play Store if you own an Android phone.
4. Search for Tor Browser by The Tor Project and install.
5. Search for Orbot by the Tor Project and install.

3. Run Orbot and just keep it running. It will help to protect your privacy.
4. Use the Tor Browser to surf the web on your cell phone.
5. When not using your cellular phone you can wrap it in aluminum foil to disable transmissions – or purchase a Faraday Cage for cellular phones.

There are many other ways to protect yourself online - but this is the bare minimal.